Static analysis

Tom Rochette <tom.rochette@coreteks.org>

November 2, 2024 — 36c8eb68

0.1 Context

0.2 Learned in this study

0.3 Things to explore

- Spectral graph theory

0.4 Tools

- Graph/tree theory
- Linear algebra

1 Overview

- Use adjacency matrices to represent a control flow graph, allows you to do operations easily (get children (nodes to which a given node may go) = $V \cdot A$, get parents (nodes from which a given node might come from) = $V \cdot A^T$ (matrix transpose))[1]

2 Basic program structure

- Fileset creation and filtering based on masks and regexes
- Initial AST construction for the fileset
- Analysis passes
- Output of diagnosis messages

3 Object analysis

- Track all properties
- Mark all properties that are read/written in each method
- Track function calls
- Track all methods signature (parameter types and return type)

4 See also

- PHP Analyzer

[1] https://www.youtube.com/watch?v=I0KXjN67hkA

5 References

- http://llvm.org/docs/Passes.html
- http://llvm.org/docs/WritingAnLLVMPass.html

5.1 Theory

- https://en.wikipedia.org/wiki/Control_flow_graph
- https://en.wikipedia.org/wiki/Loop-invariant_code_motion
- https://en.wikipedia.org/wiki/Dominator_(graph_theory)
- https://www.youtube.com/watch?v=I0KXjN67hkA
- http://www.viva64.com/en/a/0045/

5.2 List of analysis

- http://www.viva64.com/en/w/